# Understanding Privileged Identity Theft

Is your biggest threat already inside your network?

ONE IDENTITY by Quest

# Introduction

What do seven of the ten largest data breaches in the 21st century have in common? Privileged identity theft, the compromise of credentials to privileged accounts, was explicitly mentioned or indicated in post-mortem reviews of these mega-breaches.[1]

In these breaches, well-resourced, external actors, some with the backing of nation states, were able to gain the credentials of users with access to privileged accounts such as administrative or service accounts enabling them to collect and exfiltrate massive amounts of data. Although difficult to quantify the impact of these breaches, the total number of records is in the billions and includes credit card details, user accounts, employee information, health records and more. By stealing the identity of a privileged user, one with access rights to administrative and service accounts cyber criminals can steal data on an industrial scale. And these mega-breaches don't include security incidents involving intentional sabotage to critical assets such as the attack on the national power grid that occurred in the Ukraine in 2015 and 2016.

This ebook will **explain why privileged identities pose such a risk to enterprises**, how they are compromised by attackers, how current methods fail to stop these threats, and **how your organization can protect itself**.


**7 of the 10**

**biggest data breaches involve compromised privileged credentials**

*1 "The 16 biggest data breaches of the 21st century" CSO Online, September 2017*



ONE IDENTITY by Quest

## The scope of the problem

According to analyst firm Forrester, 80% of security breaches involve privileged credentials[2].The table below contains some facts about some of the mega-breaches. These are textbook cases of targeted attacks or advanced persistent threats (APT) in which criminal's targeted organizations for a specific purpose.

### Large web services provider

A couple of years ago cybercriminals gained a foothold and remained in one of the largest web services provider's environment for nearly two years ultimately resulting in the exposure of more than a billion user accounts. According to the FBI, the initial breach that led to the exposure of accounts likely started with the targeting of a "semi-privileged" employee using social engineering or spear phishing. The breaches resulted in hundreds of millions of dollars decrease in the provider's valuation.

### International e-commerce company

In the mid-2010s an international e-commerce company announced, "Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to our corporate network." The company asked all its 100+ million users to change their passwords. The company didn't provide any details about the attack but given the size of the breach and the "small number of employee login credentials" compromised, security experts suspect that attackers gained access to privileged accounts.

### US Retail chain

Cybercriminals compromised the account of a 3rd party contractor with access to the retail chain's corporate network. The intruders were ultimately able to take over several servers and install malware on Point of Sale (PoS) terminals in the stores. The result? 100 million customers' credit card details were stolen. In the aftermath, the company CEO resigned and the company has stated cumulative costs approached a total of $300 million.

### Multinational financial services company

Hackers compromised an employee's computer. From that initial intrusion they successfully obtained the highest level of administrator privileges and could take control of approximately 100 servers. The breach compromised more than 50 million household and millions of small business accounts.

### US Federal Government Agency

This breach began in the early 2010s but was not detected until two years later. The attackers stole personal information of millions of federal employees. The background investigation reports often included extremely sensitive information, including details of sexual behavior, extra-marital affairs and financial problems due to gambling. The CIA ended up pulling several officers from its embassy in Beijing in the wake of the breach. Furthermore, no one knows whether the hackers granted security clearances to people, who might work for the attackers.

### Digital media service provider

A few years ago, the provider confirmed that an external intrusion had occurred in its network and the personal information of more than 100 million subscribers, including real names, addresses, account logins and passwords, birthdays, and e-mail addresses were involved. The breach resulted in a 3-weeks closure of the provider's service. The company estimated the total cost of the data breach in the range of $150-200 million.

### Large health insurance company

The company revealed that a hacker attack exposed the data of tens of millions of current and former health plan members. The breach, in which the attacker utilized at least 50 accounts and compromised near 100 systems, began with a phishing email.

**The company committed to make significant security enhancements** in the value of more than $250 million.

*2 "The Forrester Wave™: Privileged Identity Management, Q3 2016*

## What are privileged identities?

Digital identity and access management (IAM) are the policies, processes, and technologies that digital businesses employ to establish identities and control access to their resources across dynamic ecosystems of value. This practice becomes more complex and riskier when applied to privileged accounts which include the following types:

### Administrative accounts

These include user accounts that are assigned to individuals with administrative roles that require elevated privileges, providing access to all standard user and privileged operations.

### System accounts

These accounts, such as root on Unix/Linux systems or Administrator on Windows systems, are embedded in systems or applications.

### Operational accounts

These include shared accounts used for administration and installation as well as service accounts (also known as application accounts) that enable remote software-to-software) interactions with other systems, or to run system services.

**Administrative accounts**

**System accounts**

**Operational accounts**

## How do attackers compromise privileged credentials?

The IT security community has come to the realization that perimeters cannot keep the bad guys out. In the age of the digital economy with public facing apps, bring your own devices (BYOD), and hybrid IT networks, the ways to infiltrate a network are almost infinite and hackers exploit these gaps in several ways.

### External Reconnaissance | Finding the right victim

**The initial target to compromise**

While examples exist of privileged users such as system administrators falling prey to attackers' social engineering exploits, it's far more likely that attackers will choose a softer initial target. Regular employees tend to be less tech savvy than IT personnel and make easier targets. Once the credentials of user account has been compromised the attackers will turn their attention to the ultimate goal, privileged accounts.

Sometimes the first point of attack **doesn't even lie within the target enterprises**.

In the Target breach, a small Heating Ventilation and Air Conditioning (HVAC) provider was given access to Target's corporate network and credentials for that company were stolen to gain a foothold. In the Office of Personnel Management (OPM) breach, the attackers compromised contractor credentials.

With the amount of information available to attackers, much of it shared by potential victims on a variety of social networks like Facebook, LinkedIn, Instagram and Twitter, it's not surprising that determined criminals are able to craft convincing messages to manipulate users. If social networks weren't enough, online forums such as Reddit and Stackexchange offer other avenues of research.

## Gaining a foothold

*Attackers employ several methods to gain access to IT environments, often using a combination of tactics to gain a foothold from where they can perform internal reconnaissance and compromise more credentials.*

### Social engineering

**Phishing and spear-phishing** - Most intrusions begin with an attempt to trick unsuspecting users into performing some action to further the attacker aims. Typically carried out through email, instant messaging or social networks, a phishing attempt will try to convince the victim to either share some valuable information (such as a login credential) or more commonly, to open a document or click on a link which enables the attacker to download and install some malware on the user's computer. Attackers involved in an APT attack rarely take an opportunistic approach such as generic phishing which contacts to a large number of recipients. Instead, they prefer to perpetrate spear-phishing attacks in which they use the information they gathered while performing research on the intended target organization and then craft emails or instant messages that appear more authentic.

### The Payload - Malware tools

In targeted attacks, the goal of the initial compromise is to install some software that can help attackers to either take over the victim's device or gather information such as credentials. Keylogger malware that records every keystroke made is ideal for this purpose. Other tools like Mimikatz and WCE can collect credential information stored locally. All of these tools are effective and easily accessible on the internet.

## Internal Reconnaissance

*Finding the keys to the kingdom.*

Once an attacker has gained a foothold within the victim's IT environment, they will perform internal reconnaissance. They will attempt to gather as much information as possible about the IT environment, mapping out the network and systems. This can be accomplished using a variety of network diagnostic tools such as ping, traceroute and netstat. DNS records and port scanners such as nmap yield very valuable information about the IT environment.

## Privilege Escalation

*Stealing the keys to the kingdom*

Armed with the knowledge of the network, an attacker can go about acquiring higher privileges with the ultimate goal of obtaining access to a domain controller. Pass-the-hash, SSH key acquisition, kernel and services exploits are three common techniques used to escalate privileges.

### Pass-the-hash

Passwords have been the bedrock of IT security for decades. When passwords are stored they can be encrypted using a one-way transformation called hash. Normally, an attacker that steals encrypted passwords needs to decrypt them to gain access to systems but this is time-consuming and difficult. On Windows machines, password hashes are cached in the Local Security Authority Subsystem (Lsass). If an attacker is able to access these hashes, particularly ones for administrator accounts, they download these hashes to gain access to other machines and systems. The attacker can authenticate on a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of the plaintext password.

### SSH key acquisition

Many organizations use the Secure Shell (SSH) protocol to remotely manage machines with Linux/Unix operating systems. SSH keys, access credentials in the SSH protocol, are commonly used for automated processes and for implementing passwordless ssh logins by system administrators and power users. Attackers will deploy malware to collect these keys, providing a backdoor through which they can access other servers and in some case compromise whole networks. SSH keys often provide root or administrator access which gives attackers the ability to install malware.

### Exploits

Exploits are programs that take advantage of vulnerabilities in applications or operating systems. These pieces of code enable hackers to take control of a computer system or allow privilege escalation. Software exploiting vulnerabilities on Linux Operating systems attempt

to give attackers super user access to target systems in the form of a root command prompt. In many cases, escalating to root on a Linux system is as simple as downloading a kernel exploit to the target file system, compiling the exploit, and then executing it[3].

On Linux systems attackers can use other techniques to exploit vulnerabilities with the SUID, set user ID, and SUDO, substitute user do, features. When not properly configured, attackers able to taken advantage these two services and establish root privileges allowing virtually complete control of the target system[13].

## How can you protect your organization against Privileged Identity Theft?

### Process Changes

One of the fastest ways to mitigate the risk of privileged identity theft is to remediate weak security practices. These are some quick wins your organization can achieve:


**Get a comprehensive and up-to-date list of privileged accounts**

As IT environments grow the number of administrative, service and other types of privileged accounts can proliferate. Enterprises running networks with thousands or tens of thousands of servers and network devices often lack an accurate inventory of these assets.

**Limit Scope for each Privileged Account**

Limit the scope across the infrastructure of any privileged account to enforce the principle of least privilege: Each account should have exactly the minimum rights required to carry out a specific task. For example, an account set up for administering an application should not have any system privileges beyond what is needed to make changes to the application's configuration and to restart the application. On a similar note, avoid enabling accounts on systems where they are not needed.

**Delete accounts and privileges that are no longer required**

Inadequate offboarding often creates a security gap where credentials exist for employees that have left the company or changed positions.

In the case of contractors, this situation may be more difficult to manage particularly if they only required access for a fixed-term project.

**Implement a formal password policy**

Companies with a mature security posture usually implement a formal password policy for privileged accounts. The policy should include changing default passwords as a matter of course and implementing strong passwords. It should also prohibit sharing of passwords for privileged accounts. These seem like obvious recommendations but companies large and small still fail to take these steps, making life easy for hackers.

**Prevent users taking short cuts**

Most users accessing privileged accounts such as administrative accounts and service accounts will do so to complete their daily tasks. Like anyone, privileged users want to work as efficiently as possible and are just as prone to the temptation of taking shortcuts when it comes to security. Educating employees on security policies and encouraging good behavior can go a long way to mitigating risks.

*3 "Evolve Your IAM Strategy For Your Digital Business", Forrester Research, Inc., August 18, 2017*

# Implementing Technologies to Strengthen Processes

## Privileged Access Management

### Password Management

The difficulty of securely managing access to privileged accounts grows with the size of an organization's IT network. Even in mid-size companies managing privileged access becomes unworkable without specialized tools. Many organizations start by implementing Password Management software specifically designed for privileged accounts. These solutions control access to privileged accounts, generate strong passwords, randomize passwords and store them in a password vault. Implementing a password management solution offers several benefits:

- **Enforcement of strong passwords** makes a hacker's task more difficult.
- **Passwords are managed in a centralized environment** which is easier to secure
- **Password management tools automate processes** making the creation and rotation of strong passwords for thousands or even tens of thousands accounts possible.
- **Password management systems can grant access to privileged accounts** for limited durations or within certain windows of time.

However, password management systems have their limitations. Once an attacker has compromised credentials to privileged accounts, they can move freely with the network. Moreover, these tools don't provide visibility into what the attackers did after they compromised the credentials. To reduce the risk of an attack involving privileged identity theft, organizations need to add depth to their cyber defenses.

### Privileged Session Management

Once an attacker has compromised privileged credentials, they can inflict enormous damage on your organization. Implementing a privileged session management solution provides a central access control point providing several benefits:

- **A central policy enforcement point** where managers can restrict user activity down to the level of commands based on predefined policies.
- **A point of integration for multiple authentication tools** including password management and multi-factor authentication tools.
- **Real-time monitoring** enabling security teams to supervise and shadow the activity of privileged users.
- **Recording of sessions providing audit trails** which can be searched to determine "who did what" on critical IT assets.
- **Dual control, referred to as Four Eyes Authorization**, in which certain actions and commands require real-time authorization by a supervisor.
- **Alerting and termination of sessions** in the event of policy violations.

Privileged session management mitigates the risk of a successful breach by hardening privileged accounts and limiting the types of assets that can be accessed and the types of commands that can be executed. It doesn't, however, detect when privileged credentials have been compromised. In recent years, new technologies leveraging machine learning and analytics have emerged to fulfill this need.

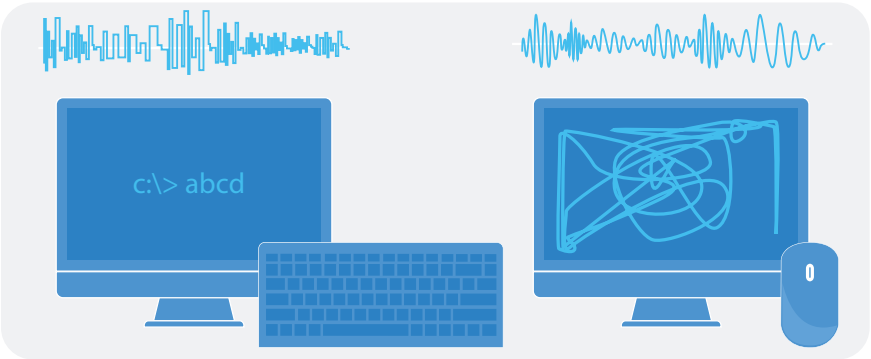
> **If a username and password is the only barrier to escalating privilege or compromising the next device, you have not done enough to stop these actors.**
>
> *Verizon Data Breach Report 2017*

## User Behavior Analytics in the context of Privileged Accounts

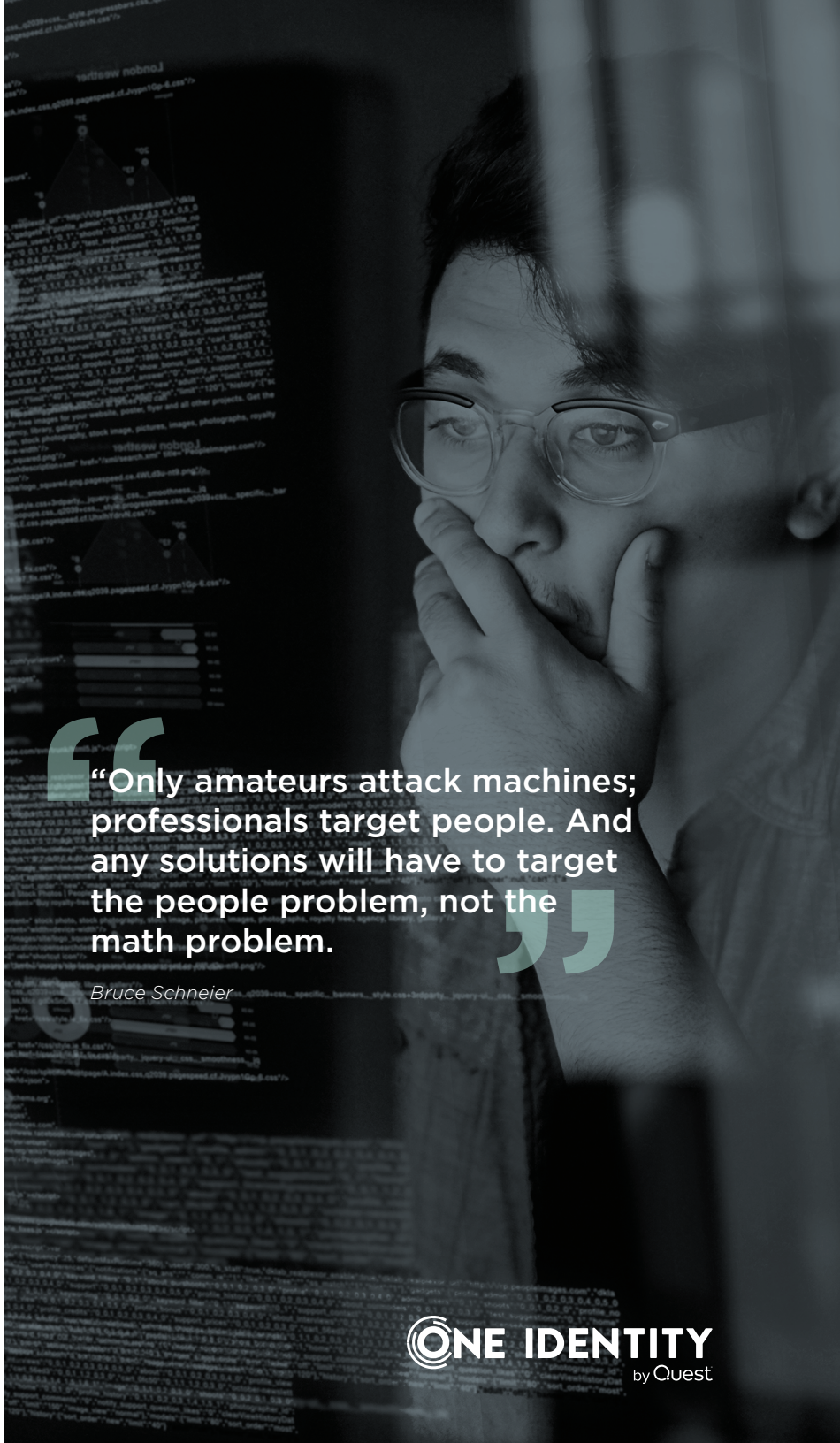
One of the challenges posed by targeted attacks is that they use unknown or “zeroday” methods and malware tools to accomplish their objective. Traditional security tools such as Security Information and Event Management (SIEM) often fail to detect these attacks because they rely on a rules-based approach. Any attack method that doesn’t fit a known pattern will not be detected. This is where User Behavior Analytics can help.

Biologists define behavior as the internally coordinated responses of whole living organisms to internal and/or external stimuli – so basically behavior is everything that we are doing consciously. Similarly, digital behavior is everything that we are doing in the digital world. Typing characteristics, screen resolution of our computer, smartphone or tablet, favorite applications or websites and many others are our digital footprints that typifies us more strongly than our habits. User Behavior Analytics (UBA) solutions are able to recognize and differentiate users based on their digital activities.

By capturing data about user behavior and applying advanced statistical techniques, UBA tools can build a baseline of normal user behavior and, through continuous monitoring of user activity, detect unusual activity. Continuously comparing actual activity to each user’s digital footprint enables behavior analytics tools to detect suspicious activity related to an attack.





This is all made possible by machine learning which provides computers with the ability to learn without being explicitly programmed. While computers are able to execute explicit, and even complex, commands at increasingly high speeds, they perform less well when used to solve problems that do not lend themselves to simple logical rules.

UBA has been used in a variety of security use cases from credit card fraud detection to rogue financial traders. Applying advanced analytics to the data captured by a Privileged Session Management tool is particularly useful for detecting privileged identity theft. Typical session metadata such as login time, session duration, location data and assets accessed provide a rich set of data to analyze but much more is possible.

## Continuous Authentication

With more detailed privileged session data, advanced analytics can detect anomalies related to behavioral biometrics. While most people are familiar with physiological biometrics such as fingerprint, iris, and retina recognition as a form of authentication, behavioral biometrics are relatively unknown. How a person interacts with a computer either through a keyboard or mouse is actually unique to that person.

Typing rhythm or keystroke dynamics analysis looks at the manner and rhythm with which a person types on a keyboard. The most typical values regarding a keystroke are dwell time (the time a key is pressed) and flight time (the time between releasing a key up and pressing the next key down).

The basic principle of mouse movement analysis is not the position of the mouse cursor, but the relative extent of the position as it changes. The most obvious factor is the speed of mouse movement. The idle time between a mouse movement and a click is as typical as the elapsed time between two clicks of a double click. What's more, the angular velocity (the rate of change of angular position of a rotating body – i.e. the mouse cursor) can be also a good characteristic.

**Behavioral biometrics** is one of the most exciting developments in IT security because it serves as a form of continuous authentication.

As we can see from the growing number of cyber-attacks, one-off authentication methods as a means of telling friend from foe have failed to provide adequate protection. Continuous authentication promises to detect privileged identity theft.

## Conclusion

Privileged Identity Theft is a widespread technique in some of the largest data breaches and cyber-attacks. A wide range of organizations have fallen victim to sophisticated, well-resourced cyber criminals but measures exist to mitigate the risks of the attack. Relatively straightforward process improvements combined with Privileged Access Management technologies such as session management and advanced analytics can help detect compromised privileged accounts and stop attackers before they are able to inflict damage on organizations.

One Identity Safeguard is an integrated solution that combines a secure hardened password safe and a session management and monitoring solution with threat detection and analytics. It securely stores, manages, records and analyzes privileged access.

Learn more about the One Identity Safeguard solutions and how they can help you prevent privileged identity theft.

## About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide.
For more information, visit www.oneidentity.com.

If you have any questions regarding your potential use of this material, contact:

**One Identity LLC**
**Attn: LEGAL Dept**
**4 Polaris Way**
**Aliso Viejo, CA 92656**

*eBook-UnifiedIdentitySecurity-KA-69156*

ONE IDENTITY by Quest